Industry Brief / Financial Services

Beyond Compliance: Why Resilience Is the Real Post-DORA Challenge

With regulatory pressure rising, financial institutions need an operating model for continuous resilience.

Point-in-Time Compliance Is No Match for Modern Risk

Financial institutions are being asked to prove resilience like never before.

They must prove not just that controls exist, but that systems will hold up under stress. Not just within discrete environments, but across cloud platforms, on-premises infrastructure, APIs, payment systems, and a growing network of third-party providers. Not just once a year, but continuously—and with evidence that stands up to regulatory scrutiny.

That's a fundamentally different way of operating, and one that traditional compliance approaches struggle to deliver.

The Digital Operational Resilience Act (DORA) brought that tension into focus. When its key January 2025 compliance deadline arrived, many financial institutions had implemented the policies, processes, and controls needed to meet foundational requirements. But maturity in core areas was far from a given. In fact, heading into DORA, **just 8% of firms reported full maturity** in resilience testing and third-party risk management.[1]

What DORA and similar regulatory shifts make clear is that a traditional, point-in-time approach to compliance doesn't scale. The requirements themselves are evolving, while the environments they apply to and the risks within them are changing constantly.

The result is a moving target: validating systems that won't stand still against requirements that won't either. Reacting to each new mandate with incremental fixes may meet near-term demands, but it does little to build lasting resilience.

For financial institutions, the new baseline is not keeping up with regulatory change, but responding to what comes next without starting over every time. That means moving beyond point-in-time validation to an operating model where resilience is built in.

90%

of financial services executives say **compliance requirements have grown more complex** in the past three years[2]

[1]"DORA European Survey – 2025 edition," Deloitte, August 2025.
[2]PwC's Global Compliance Survey 2025, PwC, February 2025.

The Path to Operational Resilience in the Enforcement Era

Here's how institutions can design once and respond many times, creating the visibility, evidence, and control needed to prove performance continuously.

Unified Visibility Across Highly Distributed Environments

Resilience starts with understanding how systems and dependencies behave in real time. In many financial institutions, that's harder than it sounds.

As financial systems and compliance functions have evolved, visibility has become fragmented across tools, teams, and environments. While this separation was once essential, it now presents significant barriers. When services span internal systems and external providers, as they often do, visibility stops at those boundaries—precisely where risk is hardest to assess.

While institutions can document controls and dependencies, they lack a clear view of how systems actually behave from end to end. The result is resilience theater: Controls are documented, but real-world performance remains largely behind the curtain.

The consequences are most apparent in real-time workflows. In areas like payment processing, where transactions move continuously across systems and third-party services, teams are left to reconstruct events after the fact instead of understanding issues as they unfold.

Addressing these gaps doesn't mean adding more tools. It means rethinking how visibility works—bringing together telemetry across network, cloud, and application environments into a unified, connected view. This allows teams to trace dependencies, understand how systems interact, and extend visibility into third-party services.

With that foundation, financial institutions can identify issues earlier, assess impact more clearly, and better understand how their dynamic systems perform in real time.

Compliance Priorities Are Expanding

Today's compliance function spans a **broad range of risk areas**, each involving distinct data, controls, and often separate systems:[3]

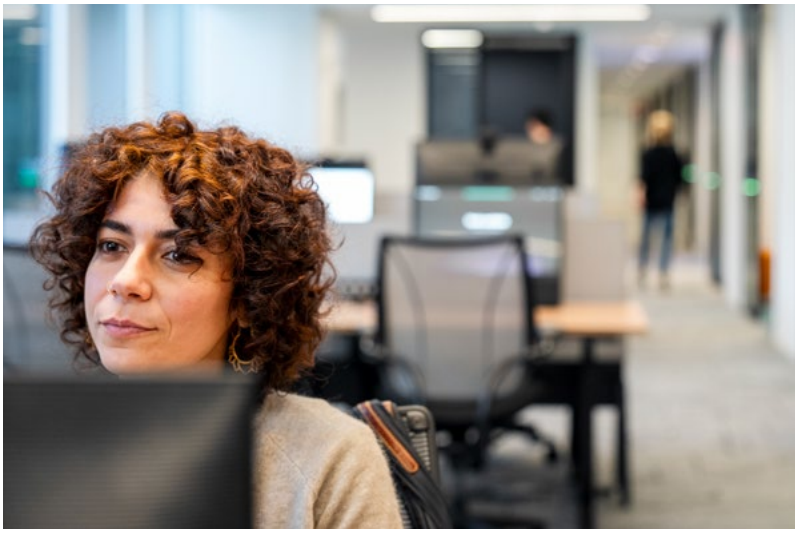
75%
Customer protection

71%
Data protection

68%
Fraud

50%
Third-party/outsourcing risk

[3]"Risky Times and Cost Pressure Call for Innovation in Bank Compliance," Boston Consulting Group, June 5, 2025.



Continuous Monitoring and Provable Resilience

Financial institutions have plenty of data about their systems. What they often lack is the ability to turn that data into proof.

When disruptions occur or regulators request evidence, producing that proof is still slow and inconsistent. Evidence must be assembled and validated before it can be trusted.

That delay is where risk accumulates. The average time to identify and contain a breach still **exceeds 240 days**—longer in cases involving third-party or supply chain compromise.[4]

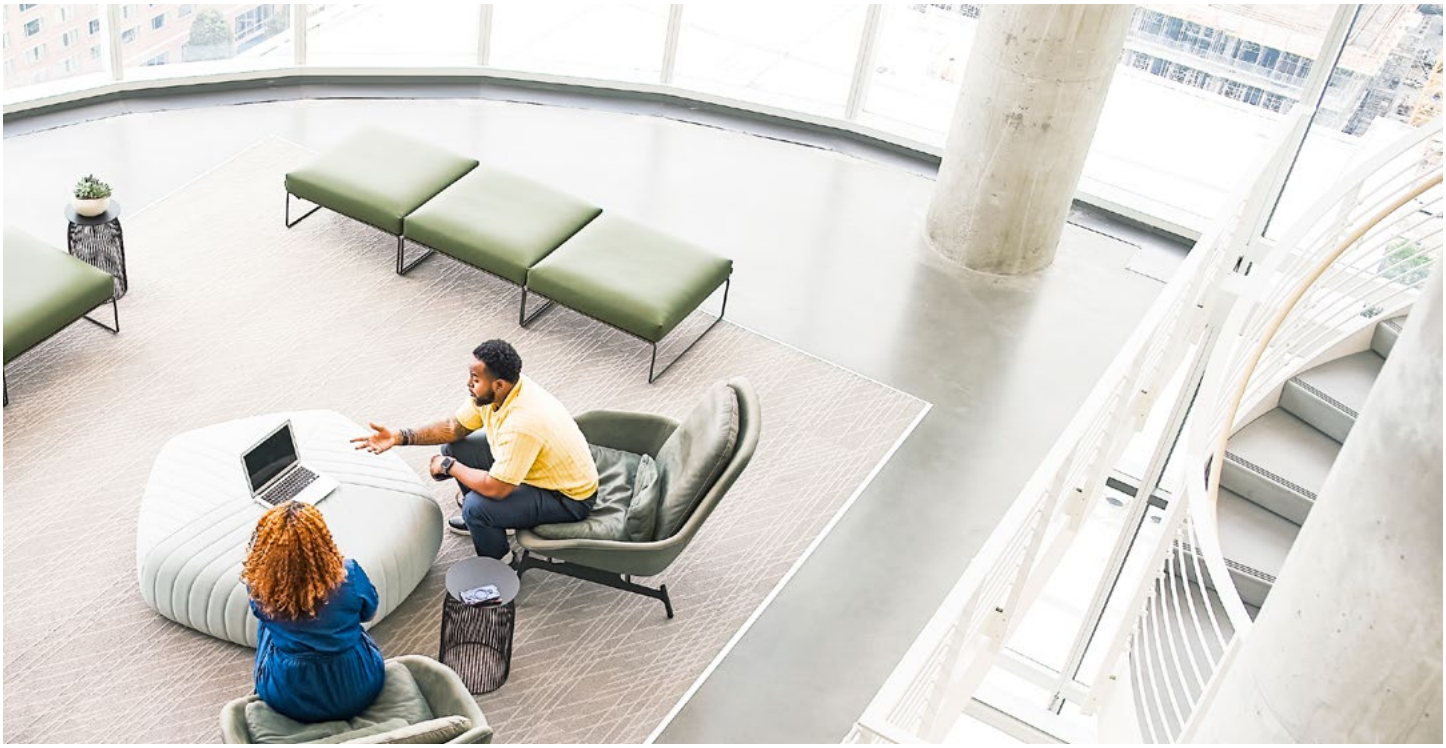
This is especially critical for financial institutions that rely on third-party dependencies, where disruptions can originate outside the organization's direct oversight. When an API provider experiences an outage, institutions must be able to demonstrate not just that the issue was detected, but how it was contained and what controls were effective.

To meet these expectations, financial institutions need infrastructure that captures and analyzes trustworthy data as a byproduct of operations. Then, instead of reconstructing events, they can readily show how their systems and controls performed and how issues were addressed at any point in time.

Achieving this requires continuously collecting and correlating system activity across environments, along with control performance and response actions. AI-driven analysis can help here, identifying patterns, validating outcomes, and surfacing risks as they emerge. Together, these capabilities create an auditable record that reflects how resilience is maintained in practice.

When that record is current and accessible, institutions no longer have to work backward to prove resilience. They have clear, defensible evidence—and a faster response to evolving risk.

4"Cost of a Data Breach Report 2025," IBM,July 2025.



Consistent Policy for Connected Architecture

If a financial institution restricts access to sensitive customer data within its core systems, that policy is clear, enforced, and regularly audited.

But the same data may be accessed through an API connected to a third-party service, where controls are applied differently. The policy exists, but it doesn't extend.

Now consider a user whose access is restricted based on role and location within a cloud environment. When that user connects through a different network path, those controls may not be applied in the same way.

This kind of inconsistency is common in financial institutions. Policies are defined centrally but enforced within individual systems. In many cases, the policies are maintained manually and updated infrequently. As users, data, and services move across cloud, on-premises, and third-party environments, the gaps become harder to track and even harder to control.

True resilience happens when your network, cloud, and security policies act as one. Controls extend beyond static rules, traveling with users, data, and services. As conditions change, enforcement adapts in real time, informed by context-aware and AI-driven decision-making.

With this approach, institutions can enforce critical requirements such as data residency and third-party risk controls, reducing compliance exposure and risk where they are most likely to emerge.

Regulatory Expectations vs. Operational Reality

Most financial institutions don't struggle to define controls. They struggle to enforce them consistently and prove they work as systems, data, and dependencies evolve.

Resilience theater replaces real performance. Controls are documented and audited, but institutions lack visibility into how systems actually behave.

Dependency mapping limits third-party oversight. Relationships across cloud, APIs, and providers are not continuously tracked, leaving institutions without a clear view of external risk.

Detection timelines undermine response. Slow identification and containment delay reporting and hinder incident management.

Fragmented tools weaken auditability. Data is spread across systems, forcing teams to assemble and reconcile evidence before it can be trusted.

Compliance is periodic, but risk is continuous. Point-in-time validation cannot keep pace with environments that are constantly changing.

From Checkbox Compliance to Continuous Resilience

DORA marked a meaningful step toward digital resilience, but it's far from the finish line. Financial institutions must move beyond point-in-time validation to an operating model where resilience is continuously visible, enforced, and proven across every system and dependency.

Cisco and Amazon Web Services (AWS) bring together infrastructure, observability, and security from core to cloud to enforce policy consistently. Together, they help financial institutions modernize core systems, streamline operations, and protect every transaction—closing the gap between compliance on paper and resilience in practice.

Build an Agile, AI-Ready Foundation

Run AI and core financial workloads reliably and flexibly across hybrid environments.

- AI-ready hybrid infrastructure for traditional and modern workloads
- Unified data and compute performance
- Secure, elastic connectivity
- Full-stack observability

Future-Proof Experiences and Operations

Deliver seamless, future-ready digital experiences while reducing operational complexity and risk.

- AI-driven operational insights and automation
- High-performance digital experiences
- Open, trusted ecosystems
- Secure global connectivity

Protect Every Transaction with Digital Resilience

Maintain trust, uptime, and compliance continuously across every transaction and channel.

- End-to-end visibility
- Zero-trust security
- AI-driven threat detection and incident response
- Audit-ready compliance controls

Powering Financial Transformation in the AI Era

Cisco and AWS deliver a unified foundation designed for the speed the market demands and the rigor the financial industry requires. Find out more about our partnership at cisco.com/go/aws.

And explore our solutions on AWS Marketplace.